

TylerHowell 4/17/2013 0:00 ** Q39 -Unable to identify manf./model of PCB, but looks like power electronics.
 *** Later identified as an Electronic Speed Controller (ESC).
 * Received more images of two more PCBs (one with enclosure), PPT presentation created to explain electronics based on scene location (1 or 2):
 * Scene 1
 ** Q178 - 2.4 GHz receiver by FlySky, model: FS-GR3E, for hobby-level RC vehicles.
 ** Q39 - Electronic Speed Controller (ESC) of unknown manf./model.
 * STVC Call with Hobbico:
 ** Confirmed that they are the seller of the Duratrax brand, including the Duratrax Spring ESC.
 ** Indicated that Q39, the blue ESC, could be from Hobby King under the brand of Turingy.
 ** Commented that transmitters from various manufacturers are typically not interoperable.
 ** Informed that the Spektrum brand is produced by Horizon Hobby.
 ** Was unaware of custom transmitter/receiver designs on the internet (checked on 4/22/2013 - there are).

TylerHowell 4/18/2013 0:00 ** Q7 - Likely sub C rechargeable battery.
 * Delivered Helion ESC exemplar to SSABT Eric Morefield.

TylerHowell 4/25/2013 0:00
 * Eric Morefield tested the inter-operability of an exemplar Fly Sky transmitter and an exemplar Spektrum SR201 receiver.

TylerHowell 4/19/2013 0:00 ** Exemplars could not talk to each other.

TylerHowell 4/20/2013 0:00 * Transmitter (likely Fly Sky) was recovered in Boston.

TylerHowell 4/22/2013 0:00 * Hobbico identified Q39 (blue PCB ESC) as a Helion Dominus ESC, which is sold by Hobby Town.
 * Ordered exemplars:
 ** 4 - Spektrum DX2E transmitters
 ** 4 - Spektrum SR201 receivers
 ** 4 - FlySky FS-GT3B transmitters
 ** 4 - FlySky FS-GR3E receivers
 ** 2 - Duratrax Spring ESC

TylerHowell 4/23/2013 0:00 ** 2 - Helion Dominus ESC

- * Received first round of exemplar transmitter/receiver
- ** Receiver is the same board revision as evidence.
- * Tested interoperability of FS Tx and Spektrum Rx
- ** Devices are not interoperable.
- * Photographed evidence and exemplars.
- * Eric Kunkel is looking into obtaining bind code for exemplars.

TylerHowell 4/25/2013 0:00

- * Eric Kunkel read EEPROM on FlySky receiver with DataIO:
- ** Only data is 6 bytes, possibly binding code.
- * Test plan:
- ** Attempt to obtain same 6 bytes off of ST microcontroller on Tx.
- ** Do differential analysis on 6 bytes in receiver with another Tx.
- ** Verify evidence Rx EEPROM status (i.e., able to be read) using xray.
- ** Read evidence Rx EEPROM, program exemplar EEPROM, test link from Tx to Rx with evidence EEPROM code.
- * Gary Baird measured RF spectrum on FlySky and Spektrum transmitters:

TylerHowell 4/26/2013 0:00 ** RF characteristics are different enough to prevent communication between systems.

TylerHowell 4/29/2013 0:00 * Datasheet for FS-GR3E receiver's RF IC obtained.

New test plan for obtaining binding code:

Bind the evidence transmitter to an exemplar receiver.

** -Verify that the handshake is one-way, and does not modify transmitter.- Verified by Tyler Howell and Gary Baird that the FS-GR3C does not transmit back a signal to the FS-GT3B.

Read the exemplar receiver's EEPROM.

Read the evidence receiver's EEPROM

** Verify the evidence EEPROM is intact and capable of being read.

TylerHowell 4/30/2013 0:00 # If the two codes match, then evidence was bound. If not, investigate further.

* Provided statement to Ed Knapp (FBI-LD-EU) on modifications to FlySky system

** Concealment mods and safety mods

* Provided Eric Morefield (FBI-LD-EU) with exemplar FS-GT3B (see inventory) for EU to test range based on various configurations of antenna and electronics location.

* Removed RF can off of exemplar FS-GT3B RF module

** A7105 tranceiver IC, unidentifiable MCU, supporting circuitry.

TylerHowell 5/1/2013 0:00 ** Removed because the bind switch does not connect to the STMicro MCU.

- * Attempted to look at transactions between Rx EEPROM and Rx MCU:
- ** MCU does not use I2C compliant signaling (i.e., ack does not get pulled to zero, only about 40% down).
- *** Jupiter I2C bus monitor did not work due to non-compliant signals.
- *** Hooked up LeCroy 104MXs-B Oscscope to clock and data lines of EEPROM.
- *** Brandon Warhurst developed a python program to parse out comma delimited ASCII files with variable

TylerHowell 5/3/2013 0:00 voltage threshold setting.

- * Parsing out I2C transactions between Rx EEPROM and Rx MCU showed two waveforms of interest:

Power on - about 25 bytes of information on bus.

Bind - about 3 bytes of information on bus.

- * Power on waveform:

*** Produced a waveform that read out all six bytes in EEPROM.

- * Bind Waveform:

** Produced when transmitter sends bind code.

** One byte of data written to EEPROM at position 0.

** Where does the other 5 bytes of data in the EEPROM come from?

- * Rx EEPROM is write protected when not in bind mode.

* Received the STmicroelectronics programmer for reading the transmitter.

TylerHowell 5/6/2013 0:00 * Power and ground pins on EEPROM have about 368 to 394 kOhm impedance measurement.

ANALYSIS EXTENT

* This test is to find out what changes are made to the EEPROM of a FlySky FS-GR3C receiver when bound to two different transmitters.

* Additionally, the test finds out what changes, if any, are made by placing an EEPROM in a different receiver and binding two different transmitters.

Eight files were created using the following naming convention:

[manf. name]_[model]_rx[rx board]-[EEPROM]-[transmitter]_[read #].bin

##. a-a-1

##. b-b-1

##. a-a-2

##. b-b-2

##. a-b-1

##. b-a-1

##. a-b-2

##. b-a-2

RESULTS

Each file contains six bytes of information

##. A954 0000 BD07

##. A954 0000 CA07

##. 2815 0000 BD07

##. 2815 0000 CA07

##. A954 0000 CA07

##. A954 0000 BD07

##. 2815 0000 BD07

##. 2815 0000 CA07

TylerHowell 5/7/2013 0:00

- * Bytes 5 and 6 in Rx EEPROM are likely the 'fail safe function' offered by FlySky
- ** The function allows for setting the trim levels of each channel to a default level if the radio link fails.

Eric Kunkel looked at the preservation of data while using programmer to talk to ST micro MCU:

- * Transmitter does not operate while hooked up to the programmer. Suggested the following procedure:

Attach SWIM connector

Connect to bench supply

TylerHowell 5/8/2013 0:00 ## Power on transmitter via the switch on the board

X-rayed receiver's EEPROM:

- * X-rays showed no breaks on die or broken wirebonds

Performed impedance check on receiver's EEPROM:

- * All pins were within nominal values of the example EEPROMs

Attempted to read receiver's EEPROM:

- * Removed EEPROM from receiver board using flux, hot air pencil - success.

- * Attempted to put EEPROM on carrier board using magnet wire for stand off (to avoid shorts by bad placement on board).

- ** Magnet wire did not provide a proper conductive path to pins of carrier board.

TylerHowell 5/9/2013 0:00 ** Will attempt to use solder bridges to connect EEPROM to carrier board.

Attempted to read receiver's EEPROM:

- * Removed EEPROM from magnet wire setup (see 5/9/2013).

- * Could not read in socket, pins were too bent.

- * Used wires and clip leads to jumper to PDIP adapter:

- ** Continuity error

- * Will attempt to solder EEPROM to carrier board.

Eric Kunkel read third TX memory:

TylerHowell 5/10/2013 0:00 * Bind codes are not in plain view.

Tx Memory:

- * Eric programmed the EEPROM on the Tx, caused no change in the Rx.

- * Program memory space of Txs are all the same, bind code likely else where on Tx.

TylerHowell 5/13/2013 0:00 * Memory does not change when power cycling device.

Rx Memory:

- * Mike Harmsen performed curve trace of EEPROM:

- ** No major irregularities on pins.

- ** Vcc, pin 8, showed that the device might have been powering up when tested.

- *** This was seen on the exemplar, but not in the amount that the evidence showed.

- ** Harmsen, Howell, and McFarlane decided to read EEPROM with DataIO

- * DataIO read:

- ** Luke Wardensky placed EEPROM on SOIC to PDIP carrier board.

- ** Tyler Howell read EEPROM using DataIO 3980xpi, Atmel 24C02A profile, PDIP socket.

TylerHowell 5/16/2013 0:00 ** Two matching reads, data placed in case's data folder along with MD5Sum hash.

Tx Memory:

- * Eric Kunkel saved evidence Tx program memroy and EEPROM to case folder:

- ** Program memory matches exemplars.

- * Tyler Howell programmed an exemplar receiver with evidence Tx bind code.

- * Tyler Howell read programmed Rx EEPROM using DataIO 3980xpi:

TylerHowell 5/17/2013 0:00 ** Bind code in evidence Tx matches evidence Rx.

- * FlySky Protocol:

- ** Internet forum: www.rcgroups.com has information on the FlySky protocol used in another product.

- ** Product uses the same A7105 transceiver IC

- *** IC has a 32-bit ID code, the A7105 ID.

- *** The A7105 ID allows for filtering of data packets.

- *** All FlySky products appear to use the same A7105 ID: 0x5475C52A (programmed to register 0x06 on startup).

- *** The A7105 ID is not the FlySky ID sent in a data packet.

- ** Forum speculates that the FlySky ID's four MSB are used to set the FH sequence.

- *** Forum speculates there are 256 sequences.

TylerHowell 5/20/2013 0:00 *** Unknown how the rest of the ID is used.

- * Started working on a 4-wire SPI parser for use with LeCroy WaveSurfer 104MXs-B oscscope.

- ** Written in Python 2.7.3, based on Brandon Warhurt's I2C python parser

TylerHowell 5/21/2013 0:00 ** Command Line Interface (CLI), inputs are CSV amplitude data points.

TylerHowell 5/22/2013 0:00 * Finalized 4-wire SPI parser for use with LeCroy WaveSurfer 104MXs-B oscscope.